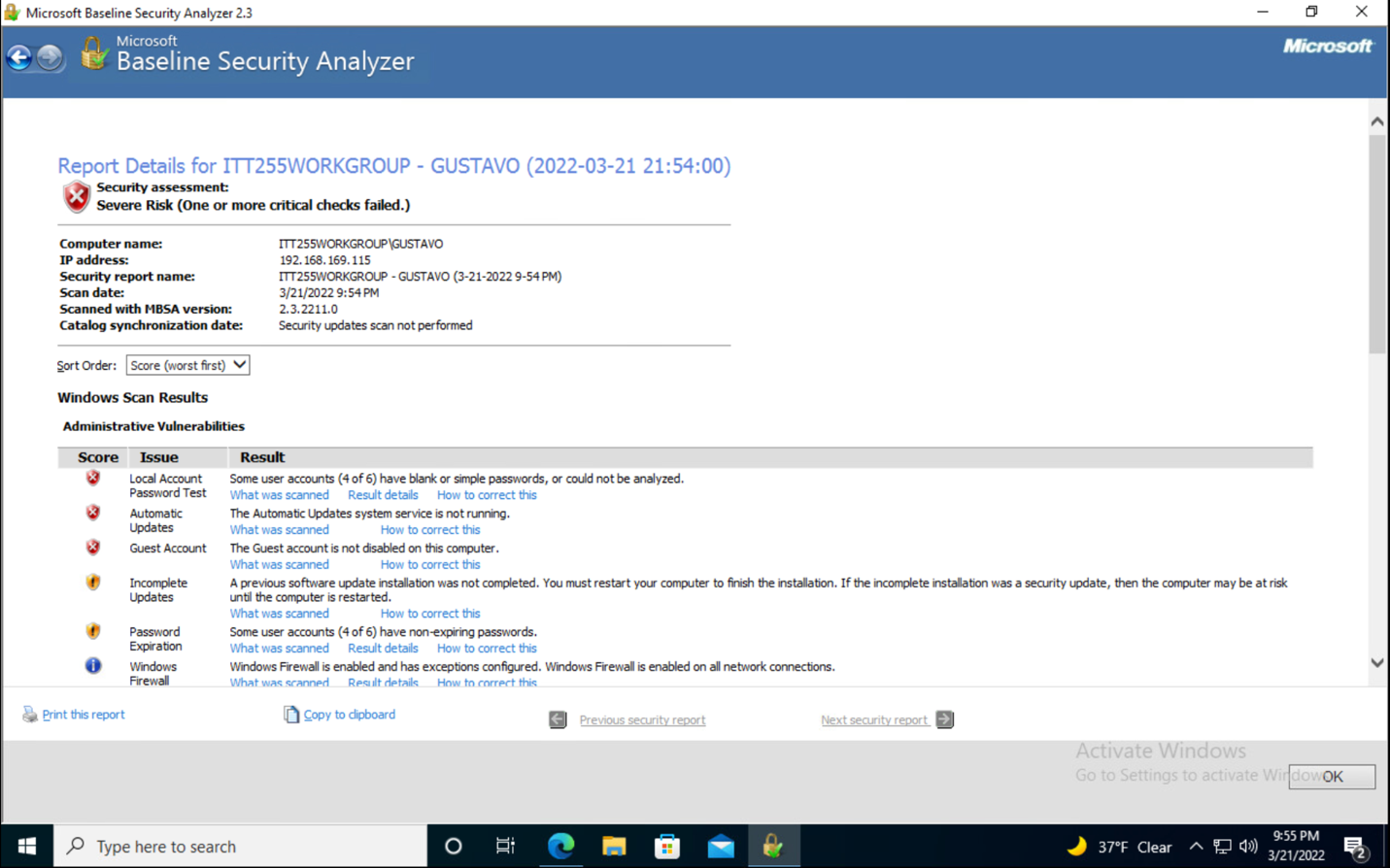
Executive Summary

In this project, we will learn to be able to use two programs, the MBSA and the Nessus. These programs will help us to be able to do a scan on our IP or local machine or any other type of IP. It is essential to remember that to do this. We must have permission. I was given four different IPs, one of which I chose was the IP 192.168.168.53 and my PC.

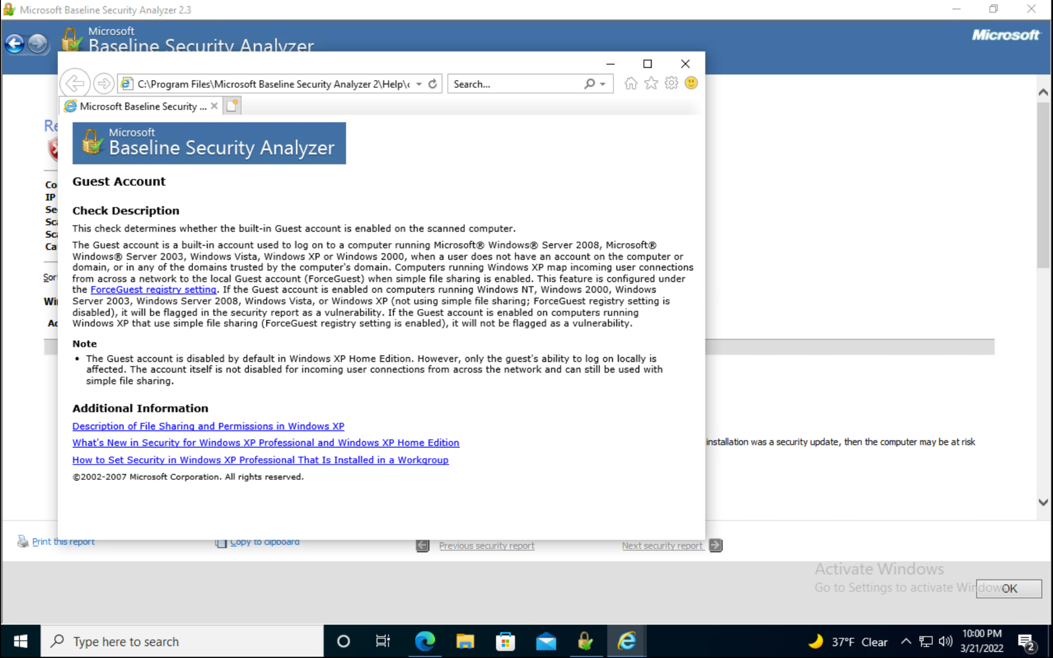
We'll start by using Microsoft's MBSA program and scanning our local machine.



We can see that after scanning our local machine, the MBSA shows three options:

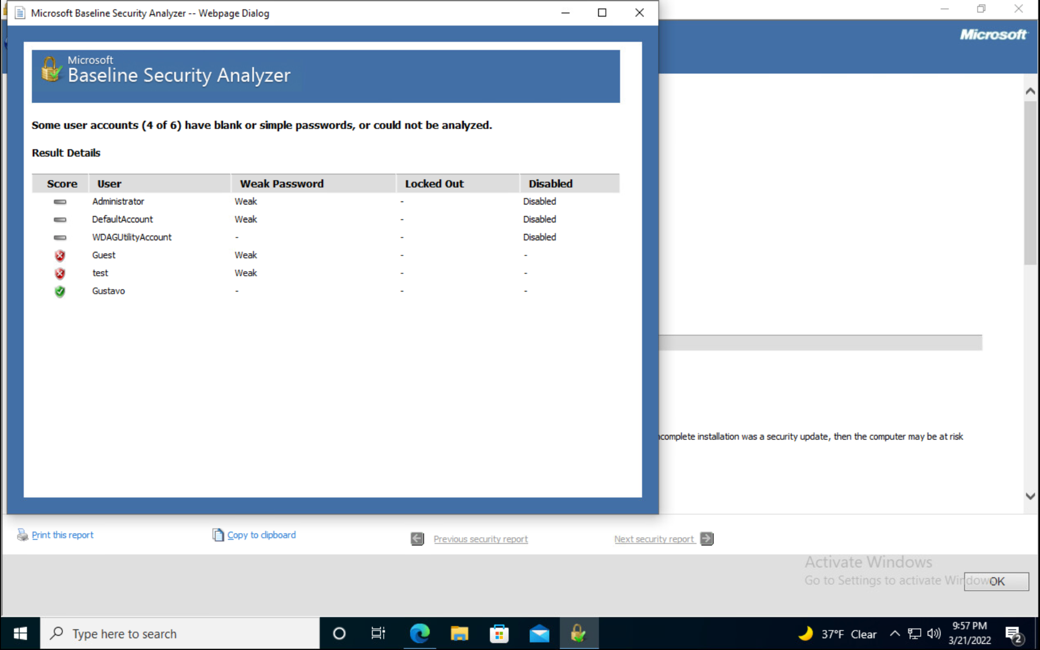
1. what was scanned

For example, in Guest Account, we can see the description of what was scanned, and it mentions that the built-in Guest account is enabled on the scanned computer.



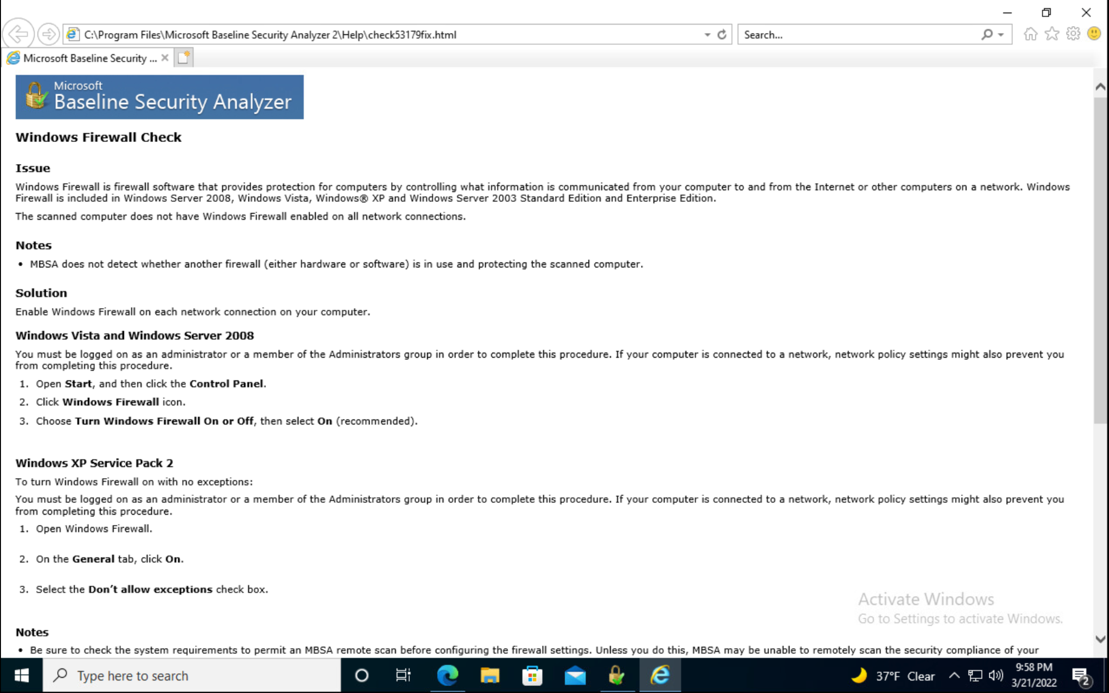
2. Result detail

For example, in the Local Account Password Test, we can see that 4 out of 6 accounts have a weak password.

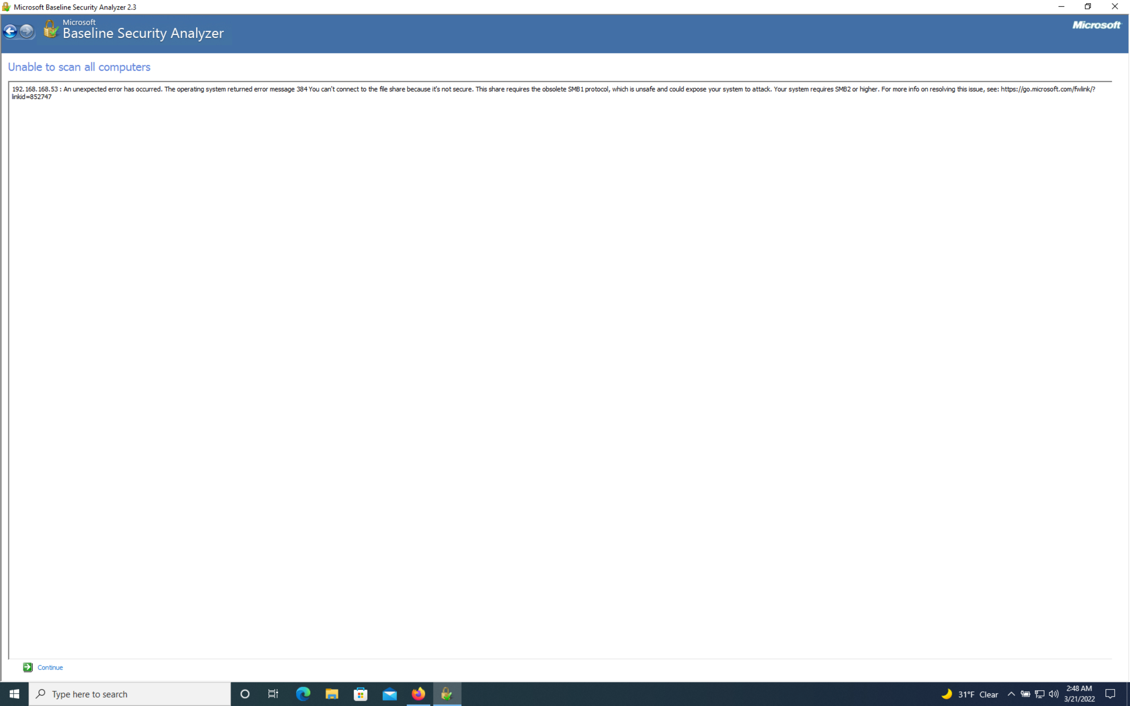


3. How to correct this

For example, Windows Firewall shows us how we can solve the problem: the firewall is not enabled in all connections. It could mean no restrictions on your computer when communicating with the Internet or other computers.



Unfortunately, the MBSA is no longer supported by Microsoft, which means no new updates for that program. We can see that it is no longer updated in the following image, it shows us an unexpected error, and the scanner cannot scan the IP 192.168.168.53.



But for our following information, we will use a new program updated and supported by the company. This program is called Nesson Professional. For this part of the project, we will use IP 192.168.168.53 to be scanned. The program offered us much more information about the vulnerabilities than the MBSA.

In this image, we can see that the program finished scanning the vulnerabilities, and it shows us as a statistic of everything it found.

We can also see in the image that the program found 69 vulnerabilities and classified them into five categories:

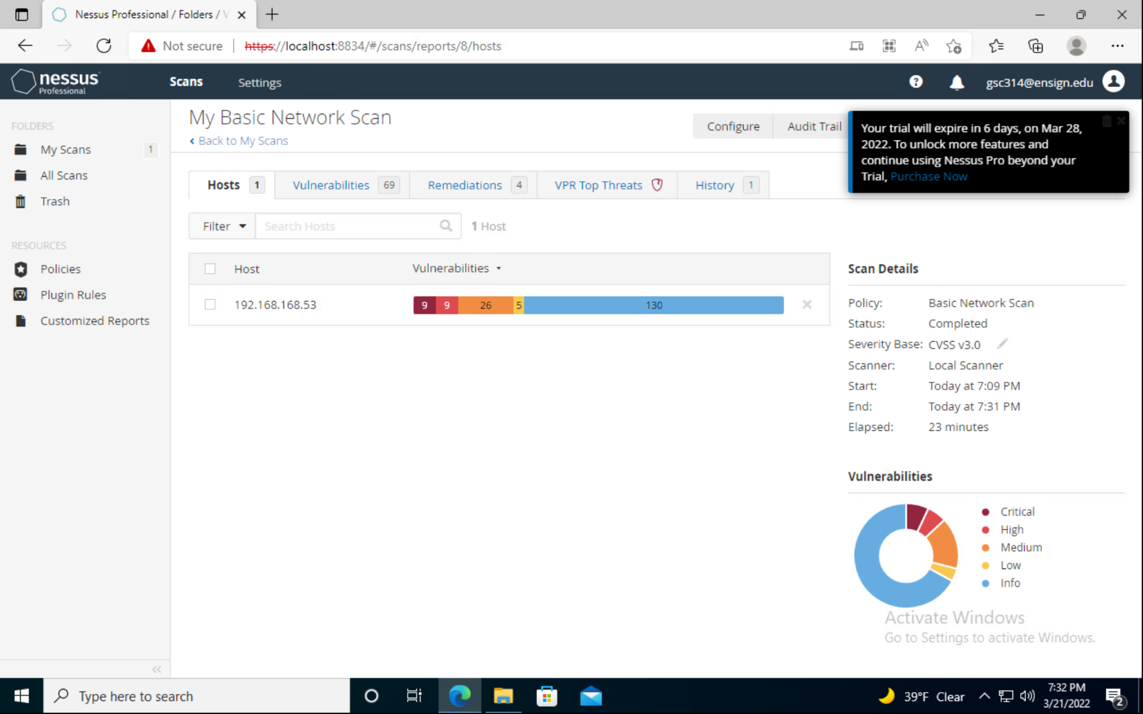
1. Critical, Nesson found 9

2. High, Nesson found 9

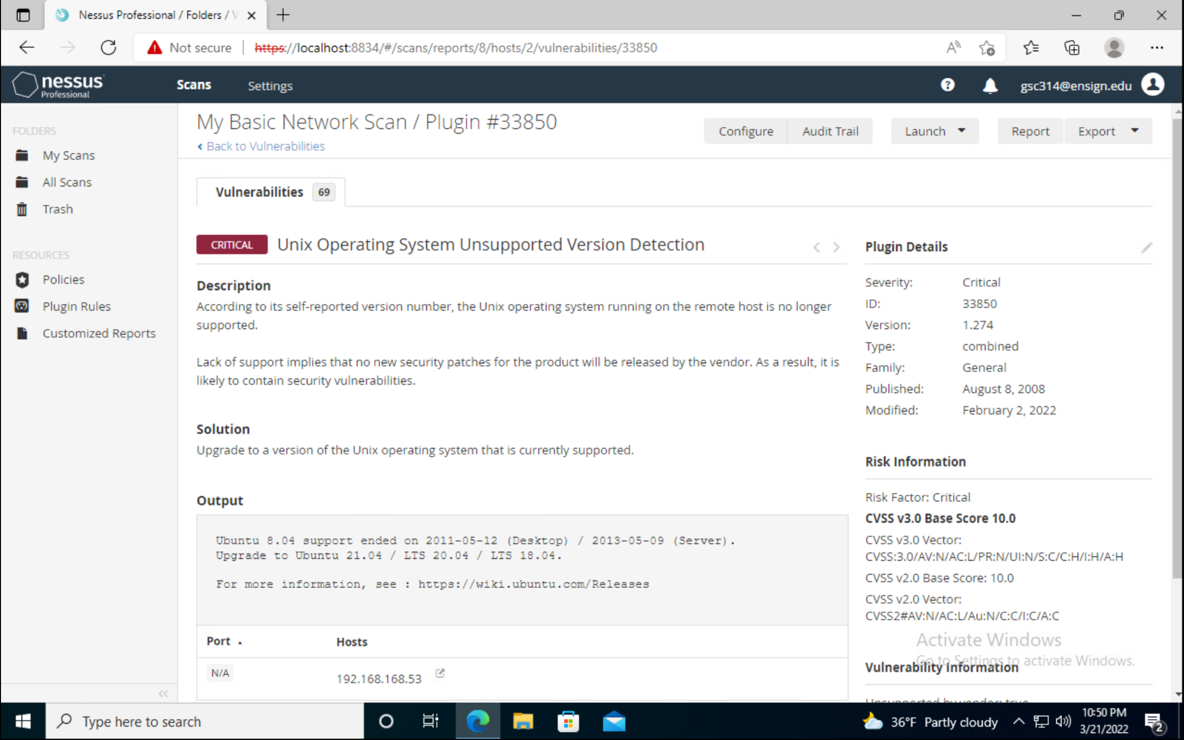
3. Medium, Nesson found 26

4. Low, Nesson found 5

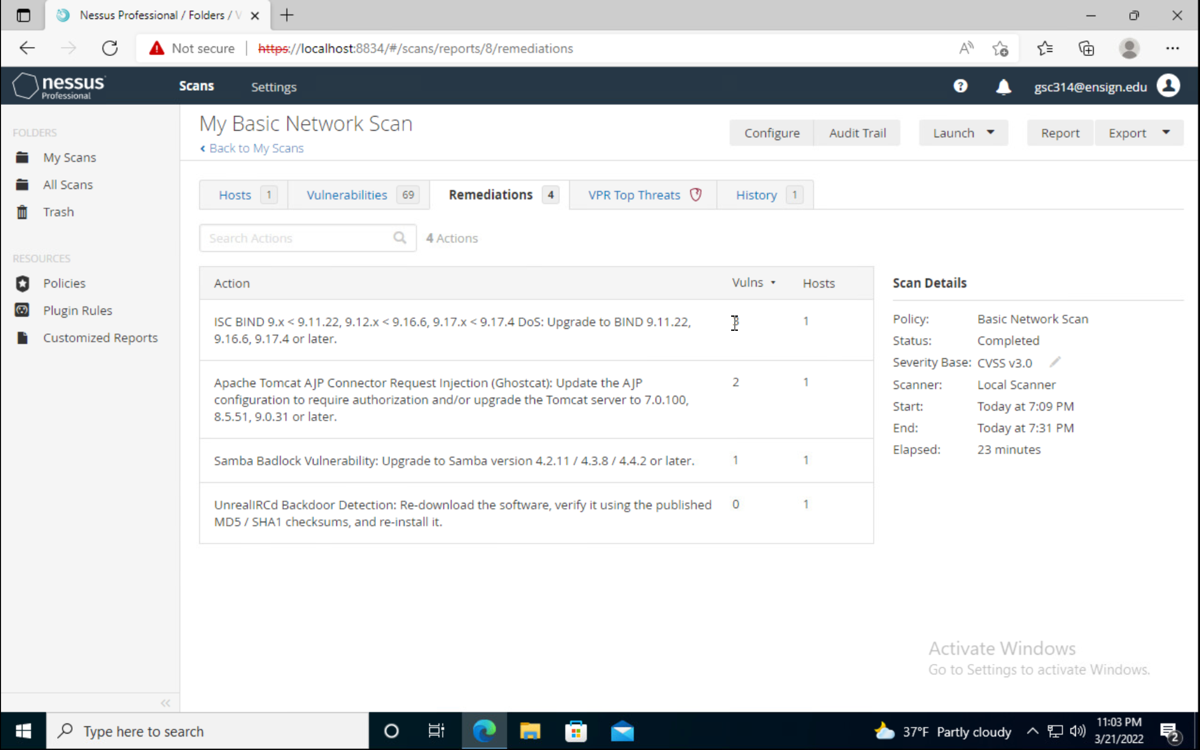
5.Info, Nesson found 130



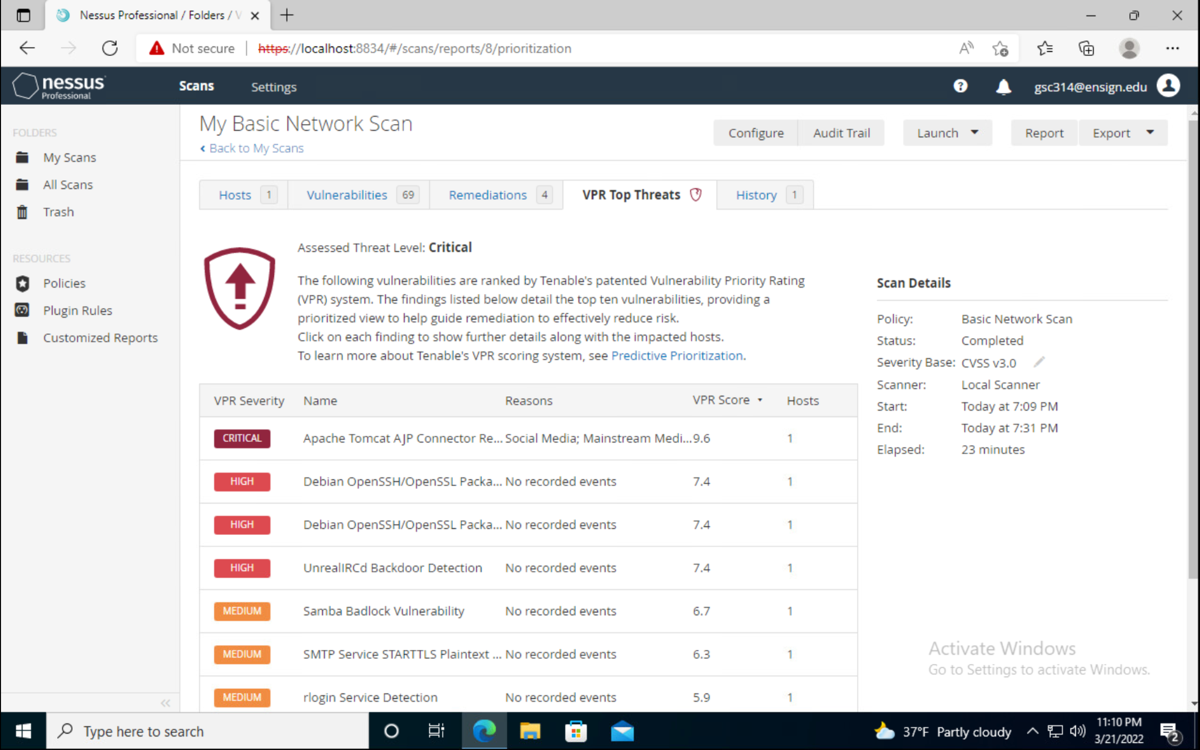
In this next image, I will show some of the critical vulnerabilities that the Nesson Pro system was able to find. We have to click on vulnerabilities 69 that was found. For example, I will use the critical one, which is that the Unix operating system is unsupported version detection.



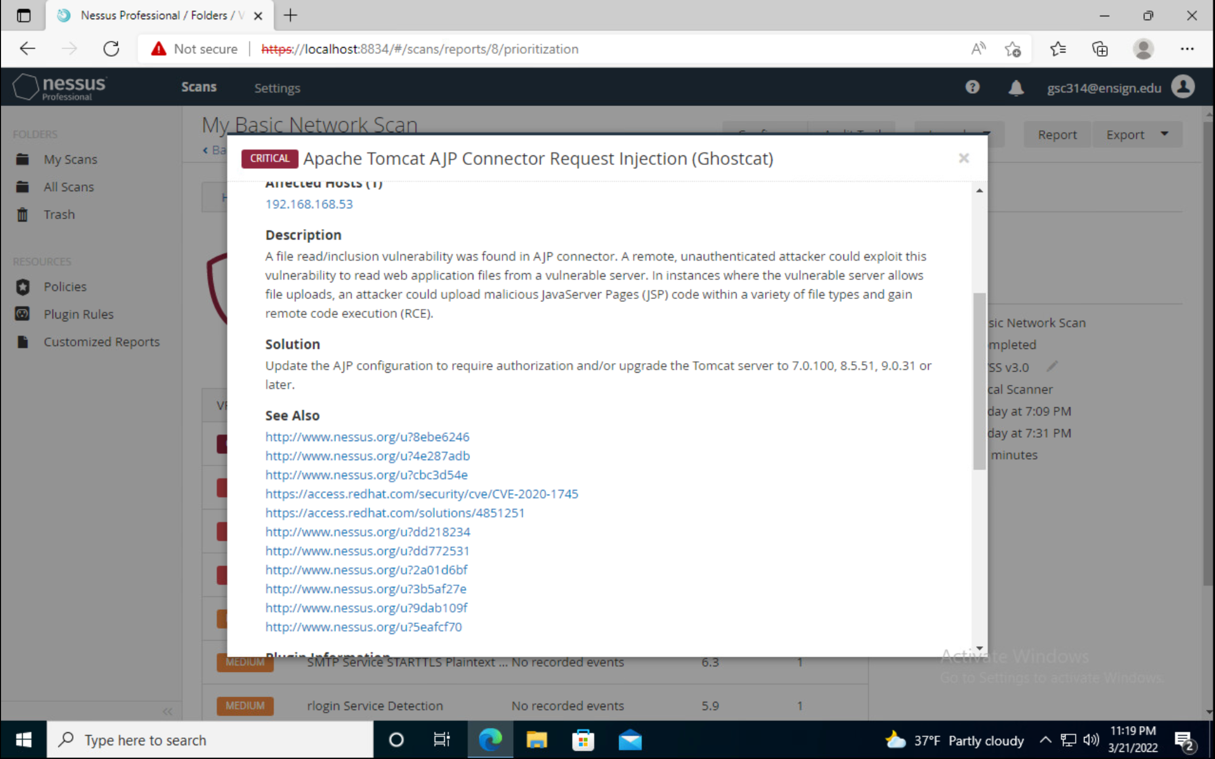
In the next part, we can see that when we click on Remediations, we can see that the program took four actions, which are to update and re-download the software.



In the last image, we must click on VPR Top threats. These will show us the TOP vulnerabilities that it could find. They are 10 TOP threats.



For example, I opened the first of the ten critical vulnerabilities, and clicking on it shows us a window, offers us the description of the vulnerability and gives us a guide to remediation or solution to reduce risk.



In this project, I learned that even the simplest things like a weak password are considered a high vulnerability. Even programs that are not updated are also a vulnerability, simply by analyzing it with the MBSA and NESSON Professional.